

### General

#### General

**Tracking ID:** 1000048227:M1  
**Last Updated Date:** 12/19/2025 4:01 PM  
**History Log:** [View History Log](#)

#### VA Team

**SOW Number:** 1000048227  
**Escalation Email Sent?:**  
**Reported via RVD:**  
**Reported via MCD:**  
**Reported via SII:** Yes  
**Issue Name:** Spring Boot Actuator Heapdump Accessible  
**Issue Description:** Actuator endpoints allow you to monitor and interact with your Spring application. Spring Boot includes a number of built-in endpoints. The springboot framework when misconfigured and bound to an interface other than localhost will allow an external threat actor to query the URI /actuator/heapdump. This can disclose sensitive information such as user credentials.  
**Issue Status:** Open  
**Issue Risk (Original):** Medium  
**Issue Number:** M1  
**Issue Risk:** Medium  
**Issue Born Date:** 6/25/2025  
**Issue Type:** I-AVM  
**Issue Born Date (International):** 25-June-2025  
**Issue Closed Date ( International):**  
**KB Reference:** CVA 0390  
**Scheduled Test Start Date:**  
**Identified by Analyst:** Peter Kasza  
**Issue Closed Date:**  
**Risk Rating Note:**  
**CVSS Score:**  
**Production Note:**  
**Affected Hosts/URLs:** http://169.177.54.144:8209/actuator/heapdump  
http://169.177.54.144:8210/actuator/heapdump  
http://169.177.54.144:8211/actuator/heapdump  
**Issue Domain:** Developer  
**Resolved Hosts/URLs:**  
**Release:**  
**Red Team Category:**  
**Red Team Root Cause:**  
**Cloud Automation Type:**  
**Cloud Root Cause:**  
**Test Case Originally Successful:**  
**Kill Chain Category:**  
**Pre-Production L2 Flag:**  
**Additional Finding:**  
**Potential L2:**

### Primary CSI ID (IT)

Application Id	Status	AVA Required	CiVA Required	Production Status
171460	Production	Y	No	Production

### Additional CSI IDs (IT)

Application Id	Tracking ID
No Records Found	

### UI ID

Version Id	Version Status	CSI Application Id	Mobile UI	UI Manager	URL Information	Web UI
No Records Found						

### PI ID - Programmatic Interface ID

PI Version ID	PI Version Name	PI Version Status	AppID	Compliance Status PI	Last Compliance Date PI	Required Compliance Test Date PI
No Records Found						

### References Section

#### Request Form Link

Tracking ID	Scheduled SOW	CWRC ID/ UI ID	Type of Test	Reason for Test	Testing Environment	Metrics & Reporting - Exception Field
No Records Found						

#### Request Form Link AVM

SOW

1000048227

#### Mobile Gateway Link

V4_Tracking ID	Tracking ID	SOW Number	Marketplace	Proposed Publish Date
No Records Found				

#### ALM Source Information Link

Tracking ID	Application Name	Component Name	Record Status	Status	Type of Scan
No Records Found					

#### Red Team Global SOW Link

Tracking ID	Scheduled SOW	Type of Test	Reason for Test	Test Status	Primary CSI ID
No Records Found					

#### ARA Request Link

ARA ID	CSI ID	Application Name	ARA SOW Status	ARA Primary Analyst	ARA Last Report Date
No Records Found					

### Level1 / Level 2 Issue Production Open/Close/Downgrade Verification

#### Open

Critical/Priority

Validator

(Reviewer):

Open Verified

Date:

Open Verified in

Production:

Could Not Be

Verified - Reasons

(OPEN):

#### Closed

Critical/Priority

Validator

(Reviewer):

Closed Verified

Date:

Close Verified in

Production:

Could Not Be

Verified -

Reasons

(CLOSED):

## Application Inventory Data.

<b>CSI_Application ID:</b>	171460	<b>CSI_Application Name:</b>	Citi Content Studio Services
<b>CSI_IS Risk:</b>	MEDIUM	<b>CSI_Production Status:</b>	Production
<b>CSI_Operating Environment:</b>	Internet	<b>CSI_Organization:</b>	ICG_Tech Cross Product
<b>CSI_Critical Functions:</b>	N	<b>CSI_Hosting Model:</b>	Hybrid
<b>Development Model:</b>	Internal	<b>CSI_SOX Indicator:</b>	Not SOX-critical
<b>CSI_Sector:</b>	ICG_Tech	<b>CSI_Vendor Package:</b>	No
<b>CSI_VA Special Grace Period Status:</b>		<b>Ownership Model:</b>	Citi Owned
<b>CIRAS Business Owner Business:</b>	Citi Markets	<b>CIRAS Business Owner Country:</b>	
<b>CIRAS Tech Owner Business:</b>	ICG Technology	<b>CIRAS Tech Owner Sector:</b>	ICG
<b>CIRAS Business Owner Sector:</b>		<b>CIRAS Business Owner Region:</b>	NA
<b>CIRAS Business Owner Unit:</b>	ICG STLT Group C		
<b>CSI_Application Manager:</b>	Nagapurkar, Mahesh (MN35732)	<b>CSI_TISO:</b>	O'Connor, Dale (D083930)
<b>CSI_GISO:</b>	Brooks, Eric (EB11836)	<b>CSI_BISO:</b>	O'Connor, Dale (D083930)
<b>CSI_ITLC Head:</b>	Kuliyev, Leonid (LK72118) G.	<b>CSI_Level 3 Head:</b>	Ambre, Milind (MA71241)
<b>CSI_Level 5 Head (SMT):</b>	Kamaldeen, Ahmed (AK37579)		
<b>AVA Required:</b>	Y	<b>CIVA Required:</b>	No
<b>CSI_AVA Exemptions:</b>	None	<b>CIVA Exemptions:</b>	

## CIVA Critical Device Inventory Information

### CIVA-CD Inventory

Inventory Tracking ID (Calculated)	Business Sector	Business	BISO	GISO	Compliance Status (Calc)	Device ID Type	Production Status
No Records Found							
<b>CIVA_Inventory Tracking ID:</b>					<b>Civa_Business Sector:</b>		
<b>Civa_Operating Environment:</b>					<b>Civa_Business:</b>		
<b>Civa_Project Name:</b>					<b>Civa_Region:</b>		
<b>Civa_GISO:</b>					<b>CIVA_Production Status:</b>		
<b>Civa_BISO:</b>					<b>CIVA_CD Device Type:</b>		
<b>Civa_RISO:</b>							

## Business Fields

**Business Fields:**

CSI Sector: ICG\_Tech

Application(s) in  
Production per  
CSI:Internet Facing  
Issue:Application(s) IS  
Risk High:Remediation  
Status: UnknownRemediation  
Status  
Comments/Next  
Steps:

Status Due By:

Building Code:

CSI Organization: ICG\_Tech Cross Product

Application(s)  
AVA Required per  
CSI:Application(s)  
Exempt per CSI:

iStatus:

Remediation  
Target Date:Remediation  
Target Date  
(Manual):Potential Head  
Start (Days):Retest Target  
Date:**Additional Business Fields**Developed and  
Supported by:Citi/Vendor  
Contact:Responsible  
Project Manager:Responsible  
Organization:

First Published: 6/25/2025 6:37 AM

CAP Summary:

IMS#:

Original Target  
Date (OTD):Corrective Action  
Description:Vendor Name (if  
applicable):Production  
Release Date:

Portal Name:

Default WVA CTI IS Staff  
Permissions: WVA CTI IS Staff - Record PermissionRevised Target  
Date (RTD):Reason for Date  
Revision:ASM Program 12/18/2025: [DH22513] Sent email that past due finding  
Status/Next requires commentary and CAP  
Steps:**Risk Information**ICAPS: VA Issue  
Type:ICAPS: CAP  
Status:ICAPS: Issue  
Detailed Status:ICAPS: Reporting  
Label-otrm:ICAPS: Effective  
Expiration Date:ICAPS: Is VA  
TestingICAPS: SOW  
#:Finding#:ICAPS: Business  
Ref:

ICAPS: CAP Flag:

ICAPS: Residual  
Risk:ICAPS: Effective  
Expiration Date  
International:

ICAPS: VA Label:

Performed:  
ICAPS: Issue  
Source Level 1:  
  
ICAPS: Issue  
Status:  
  
ICAPS: Order of  
Precedence:  
  
ICAPS: ITPSE -  
Exception Status:

ICAPS: Issue  
Source Level 2:  
  
ICAPS: Reporting  
Label:  
  
ICAPS: ITPSE -  
Exception  
Detailed Status:

### Test Information

Scheduled SOW:  
  
Business Sector: ICG\_Tech  
Business Group:  
Business:  
  
GISMR Sector: ICG  
  
Region: NA  
Preliminary  
Report Date:  
  
Incomplete  
Report Date:  
  
Project Name:  
  
Business Sector  
(Manual):

Tracking ID R&R:  
  
Type of Test: Application Vulnerability Monitoring (AVM)  
Reason for Test: Systemic Issue Identification (SII)  
  
Vulnerability  
Assessment  
Service:  
  
Testing  
Environment:  
  
Test Status:  
  
Preliminary  
Report Date(  
International):  
  
Incomplete  
Report Date(  
International):  
  
Environment:

### M&R Exception

Metrics &  
Reporting -  
Exceptions Field  
1:  
  
Metrics &  
Reporting -  
Exception Field :  
  
Metrics  
Comments:

Metrics  
Exception Update  
Date:

### Production Change Verification (PCV)

**\*\*Please note, all findings must have a successful retest before submitting PCV request.**

PCV: In Scope for No  
PCV:  
PCV: Compliance 6/25/2025  
Period Start Date:  
  
PCV: Due Date: 10/23/2025  
  
PCV: Status: Not Applicable  
  
PCV: Request  
Status:

PCV Out of Scope  
Override:  
PCV: Non  
Production  
Testing Detail:  
PCV: Elapsed 91  
Time In Days:  
PCV: Change  
Control System:  
PCV: Change  
Number:

**PCV Approval**

Date:

**PCV Link**

PCV Tracking

ID	Change Type	Other System Number	SME Reviewer
----	-------------	---------------------	--------------

No Records Found

**Issue Transfer**

Would you like to request an transfer of ownership for this issue?: No

**Issue Transfer Attachements**

Name	Size	Type	Upload Date	Downloads
------	------	------	-------------	-----------

No Records Found

Please Attach Any Relevant Approvals, Documents or Emails related to this Transfer Below:

**Issue Transfer Comments**

Comment	ID	Timestamp
---------	----	-----------

No Records Found

**Permission Fields**

<b>Inherited Permissions:</b>	Brooks, Eric (EB11836) Nagapurkar, Mahesh (MN35732) O'Connor, Dale (DO83930) WVA CTI IS Staff WVA CTI IS Staff - Record Permission	<b>Static Build Integration Record permission:</b>
<b>AVM Permission:</b>	Brooks, Eric (EB11836) ICG VA Governance Nagapurkar, Mahesh (MN35732) O'Connor, Dale (DO83930) Twaronite, Joseph (JT49670) WVA Citi All Data User WVA CTI IS Staff WVA CTI IS Staff - Record Permission	
<b>Additional Permissions:</b>	Kakkad, Aman (AK13941) Kather Mohaideen Meeran, Peer Mohamed (PK48949) Kormanik, Edward (EK00731) Packirisamy, Ramesh (RP76168) Webservices, ApScanArchBdgPRD (ApScanArchBdgPRD)	<b>Report Permissions:</b>

**Root Cause Determination****Root Cause Analysis**

RCD: In Scope For No RCD Override: No

RCD:

RCD: Submission

DueDate:

RCD: Approval

DueDate:

RCD: Elapsed time: 0

RCD Link

RCD Submission Status: Not Applicable

Tracking ID	Source of Issue	Type of Change	Which category do you believe caused the finding in the first place	What can be done to prevent this from occurring in the future? Please provide specific details	VA Retest Requests (RCD Link)
No Records Found					

### Metrics Fields

#### Compliance Info

Compliance Tracking Date:

Compliance Tracking Date (Calculated): 6/25/2025

Issue Moved Date:

Aging Range: 

Compliance Tracking Date Calculated International: 25-June-2025

Compliance Status : Past Due

Elapsed Time: 211

Issue Aging: 211

Preliminary Report Date (1st SOW):

Preliminary Report Date (1st SOW)( International):

Incomplete Report Date (1st SOW):

Incomplete Report Date (1st SOW)( International):

KB Reference #: CVA 0390

Business Sector (metrics): ICG

Monthly IS Report Business:

Monthly IS Report Aging Category: 181 - 364

Monthly IS Report RR Business Sector:

Monthly IS Report New Existing: EXISTING

#### Metrics Section

AVA Required Change Date(CSI):

Go Live Date:

Issue Risk (new): 4 - Medium

Go Live Date(1st SOW):

Issue Remediation Date:

New Application Or Functionality: No

Issue - Days Past Due (Remediation Date SBT): 0

New Application Or Functionality Override:

Go Live Date - Finding Level

Type Of Scan:

<b>Override:</b>		<b>Original Issue Tracking ID:</b>	
<b>Re-Opened Issue Check:</b>		<b>Hybrid Cloud Medium Issue Count:</b>	0
<b>Hybrid Cloud High Issue Count:</b>	0	<b>Original Go Live Date Check:</b>	
		<b>Original Prelim Date Check:</b>	
		<b>Original Incomplete Date Check:</b>	

CIRAS Feed Fields			
<b>CIRAS Feed Required (IT):</b>	Yes	<b>VA Source Type:</b>	AVA
<b>CIRAS SOW:</b>	1000048227	<b>CIRAS Primary Resource ID - TEST:</b>	
<b>CIRAS Primary Resource ID:</b>	171460	<b>CIRAS Test Type:</b>	Application Vulnerability Monitoring (AVM)
<b>CIRAS Primary CTC Version ID:</b>		<b>CIRAS UI/ID:</b>	
<b>CIRAS Primary Critical Device ID:</b>		<b>CIRAS Issue Status:</b>	Open
<b>CIRAS Primary CSI Production Status is Retired?:</b>		<b>CIRAS Primary CTC Version ID Override:</b>	
<b>CIRAS Issue Status Override:</b>			
<b>CIRAS Feed Required (IT) Override:</b>			
<b>SecOps Comments:</b>			

### Instance Tracking

WVA Instances tracking (Issue Tracking Module Reference Number)			
Tracking ID	Instance ID (SOW# issue# : instance#)	Instance Status	RCE
No Records Found			
<b>Aggregate of Instance (ALM):</b>		<b>Aggregate of Open Instances:</b>	
<b>Aggregate of Closed Instances:</b>			

### Additional Issue Information

Fields to Evaluate		
<b>VA Backdoor Finding:</b>	<b>Issue Detailed Status:</b>	
	<b>Issue Count (Calculated):</b>	Medium - Open

**Issue** Please disable or restrict access to the heapdump actuator.

**Recommendation**

:

**Affected**

**Resources:**

**Scan Type:**

### VA Knowledge Base

System Tracking ID

No Records Found

**CVM\_High\_CVE\_Instances:**

**CVM\_Medium\_CVE\_Instances:**

**CVM\_Issue\_Due\_Date:**

**CVM\_Issue\_TrackingID:**

**CVM\_Vulnerable\_Library:**

**CVM Issue Status:** Open

**CVM\_Component\_Active:** Yes

**RCE:**

**Program Issue Risk:** Level 4

**CVM\_CVSS\_Score:**

**CVM\_Policy\_Impacted:**

**CVM\_SCORE\_CAT:**

**Tool\_Risk\_Rating:**

..

**Attack Complexity:**

**Level of Authentication Needed:**

**Confidentiality Impact:**

**Confidentiality Requirement:**

**Integrity Impact:**

**Availability Requirement:**

**Availability Impact:**

**Integrity Requirement:**

**Collateral Damage Potential:**

**Target Distribution:**

**Availability of Exploit:**

**Type of Fix Available:**

**Related Exploit Range:**

**Level of Verification that Vulnerability Exists:**

**Issue Identification Process:** VA

**Issue Source System:** Archer WVA

**Asset Inventory:** CSI

**Resolution Short Description:**

**ICAPS: Submitted Date:**

**ICAPS: Submitted Date(International):**

## ISO VA Issue Tracking

### ISO Additional Details

**Remediation**

**ISO Status:**

**Owner:**

**IAM Remediation**

**Owner (Cloud**

**Only)::**

**ISO Comments:**

Copyright © 2010 EMC Corporation. All Rights Reserved